AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) Method for device-type authentication in a communication system, comprising the steps of:

providing, in a first device connected to said communication system, first header information of a communication message;

said first header information being related with a device-type associated commitment;

said device-type associated commitment being a commitment for devices of a particular device-type regarding what capability the devices support;

tamper-resistantly creating a first signature in said first device based on at least tamper-resistant device-type specific information of said first device;

providing, in said first device, second header information of said communication message comprising said signature;

communicating said communication message to a second device connected to said communication system; and

authenticating said first header information by verifying said first signature after said communicating step,

wherein said step of authenticating in turn comprises:

determining, in said second device, a device-type of said first device based on said first header information;

creating a second signature in said second device based on at least tamper-resistant information associated with said determined device-type; and

accepting said determined device-type as authentic if said first and second signatures agree..

2. (original) Method according to claim 1, wherein said communication system is based on a transfer protocol selected from the group: of HyperText Transfer Protocol and Simple Mail Transfer Protocol.

3. (original) Method according to claim 2, wherein said device-type associated commitment is a commitment to follow Digital Rights Management compliance.

4. (original) Method according to claim 1, wherein said first device is a user terminal.

5. (original) Method according to claim 1, wherein said second device is a server.

6. (original) Method according to claim 1, wherein said device-type specific information comprises a definition of an algorithm according to which said signature is to be created.

7. (original) Method according to claim 1, wherein said device-type specific information comprises a data string being unique for each particular device type.

8. (original) Method according to claim 1, wherein said step of creating a signature is additionally based on at least one item in the group of: time, date and header information.

9. Canceled.

10. (currently amended) Method for device-type authentication in a communication system, comprising the steps of:

providing, in a first device connected to said communication system, first header information of a communication message;

said first header information being related with a device-type associated commitment;

said device-type associated commitment being a commitment for devices of a particular device-type regarding what capability the devices support;

tamper-resistantly creating a first signature in said first device based on at least tamper-resistant device-type specific information of said first device;

providing, in said first device, second header information of said communication message comprising said signature;

communicating said communication message to a second device connected to said communication system; and

authenticating said first header information by verifying said first signature after said communicating step~~Method according to claim 1~~,

wherein said step of authenticating in turn comprises ~~the steps of~~:

forwarding information about said first header information and said first signature from said second device to a third device connected to said communication system;

requesting a verification of the authenticity of said first header information by said third device; and

accepting said first header information as authentic if said third device provides a positive verification.

11. (original) Method according to claim 10, wherein said third device is associated with a manufacturer of said first device.

12-15. Canceled.

16. (currently amended) Communication device connectable to a communication system, comprising:

a communication interface for receiving a communication message from a sending device connected to said communication system;

said communication message comprising first header information being related with a device-type associated commitment;

said device-type associated commitment being a commitment for devices of a particular device-type regarding what capability the devices support;

said communication message further comprising second header information in turn comprising a first signature; and

authenticating circuitry arranged to verify said first signature,

wherein said authenticating circuitry comprises:

circuitry arranged to determine a device-type of said sending device based on said first header information;

storage for storing device-type specific information of communication devices;

a signature generator arranged to retrieve device-type specific information corresponding to said determined device-type;

said signature generator being further arranged to create a second signature based on said retrieved device-type specific information; and

circuitry arranged to accept said determined device-type as authentic if said first and second signatures agree.

17. Canceled.

18. (currently amended) Communication device connectable to a communication system, comprising:

a communication interface for receiving a communication message from a sending device connected to said communication system;

said communication message comprising first header information being related with a device-type associated commitment;

said device-type associated commitment being a commitment for devices of a particular device-type regarding what capability the devices support;

said communication message further comprising second header information in turn comprising a first signature; and

authenticating circuitry arranged to verify said first signature~~Communication device according to claim 16~~,

wherein said authenticating circuitry ~~comprises~~is arranged to:

~~means for forwarding~~ forward information about said first header information and said first signature to a further device connected to said communication system;

~~means for requesting~~ request a verification of the authenticity of said first header information by said further device; and

~~means for accepting~~ accept said first header information as authentic if said further device provides a positive verification.

19. (previously presented) Communication device according to claim 16, wherein said communication interface is arranged to support a transfer protocol selected from the group: of HyperText Transfer Protocol and Simple Mail Transfer Protocol.

20. (original) Communication device according to claim 19, further comprising Digital Rights Management means, whereby said device-type associated commitment is a commitment to follow Digital Rights Management compliance.

21. (previously presented) Communication device according to claim 16, wherein said communication device is a server.